UNIVERSITY OF OKLAHOMA
Health Sciences Center
Information Technology

Email Transmission and Use Policy

1. Purpose

This University of Oklahoma Health Sciences Center (OUHSC) Email Transmission and Use policy establishes the rules for using OUHSC email to send, receive, or store electronic mail and informs email users of their responsibilities associated with such use. This policy applies to all Workforce Members and individuals granted access privileges to OUHSC Information Systems with the capacity to send, receive, or store electronic mail.

2. University Business[1]

All University Business that is conducted on email is to be done only through the OUHSC-provided email system, which may include a University-approved patient portal and/or an OUHSC-assigned email account. Workforce Members (faculty, staff, students, residents, trainees, volunteers) and affiliates who have OUHSC email accounts **shall not use personal email accounts or non-University email systems to conduct OUHSC Business**.

3. Auto-forwarding or Auto-redirecting Email Messages

Workforce Members must not auto-forward or auto-redirect their OUHSC email to non-University provided systems. Examples of non-University provided email systems include, but are not limited to, OMRF, VA, Gmail, Outlook/Hotmail, Yahoo, AOL, and email provided by other Internet Service Providers (ISP) such as Cox or ATT.

4. Authorized Recipients

Workforce Members may send OUHSC email to authorized internal and external (subject to encryption requirements) recipients for authorized purposes. For example, PHI may be sent only to authorized recipients and only for treatment, payment, or health care operations purposes. Users may send ePHI to third parties with whom the University has a Business Associate agreement in place (contact Purchasing or the Office of Research Administration to confirm Business Associate status of a particular vendor or sponsor). Student records subject to FERPA may be sent only to University officials who have a legitimate educational purpose and others authorized by law.

5. Encrypted Transmission of Confidential or Regulated Email Outside OUHSC

If confidential or regulated University information, such as PHI or confidential research data, must be transmitted over an external network (e.g., the Internet), the email communication channel and/or the email message must be encrypted. Message encryption options include typing [secure] in the email subject line, using the Secure Email plugin, or using a University-approved Patient Portal. (For additional policy regarding sending PHI via email, refer to HIPAA Privacy Safeguards policy. For a list of business partner email domains using encrypted communication channels see the TLS link on the Secure Email web page[2].)

[1] University Business: Work performed as part of an employee's job responsibilities, or work performed on behalf of the University by faculty, staff, volunteers, students, other trainees, and other persons whose conduct, in the performance of work for the University, is under the direct control of the University, whether or not they are paid by the University. University business includes the use of a Portable Computing Device to access OUHSC email, non-public University systems, networks, or data in the performance of work for the University.

[2] http://it.ouhsc.edu/services/infosecurity/SecureEmail.asp

6. Portable Computing Devices

To protect confidential and regulated University information that resides within the OUHSC email system, Portable Computing Devices that connect to the OUHSC Exchange environment are required to be encrypted and to have baseline security settings applied. See the OUHSC IT Portable Computing Device Security policy for these requirements.

7. Confidentiality Notice

Emails that contain confidential University information, such as PHI, or regulated data must include a confidentiality notice in the signature block, such as: *Confidentiality Notice: The information contained in this message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure, distribution, or retention is strictly prohibited. If you are not the intended recipient or believe that you have received this message in error, please notify the sender immediately by reply email and permanently delete the original message.*

8. Email Privacy

All OUHSC email content and systems are owned by the University; as such, all user activity is subject to logging and review. OUHSC email may be subject to release under the applicable law. OUHSC email is subject to open records requests. Refer to the IT Acceptable Use policy for additional information.

9. Scope

This policy applies to all Workforce Members and individuals granted access privileges to OUHSC Information Systems with the capacity to send, receive, or store electronic mail.

10. Regulatory References

- HIPAA Standards for Safeguarding Customer Information, 164.308 (a)(ii)(B), 164.308 (a)(4)(i), 164.308 (a)(4)(ii)(C), 164.308 (b)(1), 164.312 (e)(1), 164.312 (e)(2).
- Gramm-Leach-Bliley Act ("G–L–B Act"), Section 501(b)
- Payment Card Industry Data Security Standard (PCI DSS)
- Family Educational Rights and Privacy Act (FERPA): 20 U.S.C. §1232g; 34 CFR Part 99
- NIST Special Publication 800-53 rev 4, SC-8 Transmission Confidentiality and Integrity
- NIST Special Publication 800-53 rev 4, SC-13 Cryptographic Protection
- NIST Special Publication 800-53 rev 4, AC-4 Information Flow Enforcement
- NIST Special Publication 800-53 rev 4, AC-20 Use of External Information Systems

11. Authorization/Enforcement

This policy is authorized and approved by the OUHSC Deans' Council and the Senior Vice President and Provost and enforced by the Chief Information Officer. Internal Audit and other authorized departments of the University may periodically assess Business Unit compliance with this policy and may report violations to the University Administration and Board of Regents.

12. Policy Maintenance

This policy is scheduled to be reviewed, updated, or modified annually or more frequently if necessary.

13. Revision, Approval and Review

13.1 Revision History

Version	Date	Updates Made By	Updates Made
0.1	02/24/2017	OUHSC IT	Baseline Version
0.2	02/24/2017	OUHSC IT	Updated Regulatory References
0.3	02/24/2017	OUHSC IT CIO	Minor changes: See SharePoint track changes
0.4	03/02/2017	OUHSC Legal Counsel (Jill Raines)	See SharePoint track changes.
.05	04/17/2017	OUHSC Legal Counsel (Jill Raines)	See SharePoint track changes.
.06	04/19/2017	OUHSC CTO	See SharePoint track changes.
.07	05/09/2017	OUHSC Information Security Review Board (ISRB)	See SharePoint track changes.
.08	05/10/2017	OUHSC IT Managers	See SharePoint track changes.
.09	05/17/2017	ISRB	See SharePoint track changes.
1.0	05/25/2017	OUHSC Deans' Council and Senior Vice President and Provost	Change "redirect" to "auto-redirect"

13.2 Approval History

Version	Date	Approved By
1.0	05/25/2017	OUHSC Deans' Council and Senior Vice President and Provost

13.3 Review History

Date	Reviewed By
04/19/2017	OUHSC IT
04/17/2017	OUHSC Legal Counsel
05/09/2017	OUHSC Information Security Review Board